Consumer Corner

by Illinois Attorney General LISA MADIGAN

Protecting Your Identity:
When Thieves Go "Phishing" for Information

Phishing is a computer-based scam designed to trick unsuspecting consumers into revealing sensitive financial information to identity thieves. Once thieves have this information, you may quickly find yourself the victim of identity theft.

***Q*. My husband received an e-mail asking him to contact his bank immediately about a problem with his account. The e-mail contained a link to the bank's Web site, where a pop-up window appeared asking that he provide his account number and password. Although the Web site looked legitimate, it seemed odd that his bank would contact him by e-mail about something so urgent, so I told him he should call the bank rather than respond to the e-mail. When he called the bank, my husband was told that there was no problem with his account and that someone must have been "phishing" for his information. What exactly is phishing, and is it common?**

***A*.** An increasing number of Illinoisans have been on the receiving end of a relatively new high-tech scam called "phishing." In this scam, con artists pose as your financial institution, your credit card provider, or even a government agency and send spam e-mails or pop-up messages designed to trick you into revealing your account information, credit card numbers, Social Security number, or other confidential information that could be used to steal your identity.

The e-mails and pop-up messages often look authentic, and they usually direct you to Web sites that look just like the sites of the legitimate businesses. Once you get to the site, you are asked for sensitive account information to "update" or "validate" your account for some urgent reason.

The most important thing to remember is that legitimate companies and banks will not ask you for personal or financial information via e-mail. If you receive an e-mail or pop-up message asking for sensitive personal or account information, do **not** reply to the message or click on any links in the message. If you are concerned about your account or if you want to check the validity of the e-mail, it is important to contact your bank or credit card provider using a phone number or Web site that you know is legitimate. If in doubt, look at your most recent bank statement or credit card bill, which will most likely include the business's customer service number and Web site address.

If you think you may be the victim of a phishing scam, contact your financial institutions immediately and close your affected accounts. If you have disclosed your account information, passwords, Social Security number, or other identifying information, you also should contact one of the three credit reporting agencies **(Equifax: 1-800-525-6285, Experian: 1-888-397-3742, TransUnion: 1-800-680-7289)** to request that an initial fraud alert be placed on your account and ask for a free copy of your credit report so you can review it for unauthorized charges or credit accounts. Additionally, you should contact my office's **Identity Theft Hotline (1-866-999-5630; TTY: 1-877-844-5461)** to find out further steps you can take to protect your identity.